

CLAIMS

What is claimed is:

- Sub
A3
- 09592322-061300
1. A method for securely transferring data between an agent and an application server through a non-secure node comprising:
 - (a) establishing a session key between the agent and the application server by utilizing a public key of the application server; wherein the public key of the application server is embedded in the agent; and
 - (b) establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non-secure node by using a relay module.
 2. The method of claim 1 wherein establishing a communication link between the application server and the non-secure node by using a relay module comprises:
 - dynamically instantiating the relay module having a first port for communicating with the application server and a second port for communicating with the agent, the relay module listening on a first predetermined port number on the first port and a second predetermined port number on the second port; and
 - the application server connecting to the first port of the relay module to establish a connection therewith.
 3. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:
 - pushing data encrypted by the established session key from the agent to the application server over the end-to-end secure connection.
 4. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:

pulling data encrypted by the session key from the application server over the end-to-end secure connection to the agent.

5. The method of claim 1 wherein establishing a session key between the agent and the application server by utilizing a public key of the application server further comprises:

establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween.

6. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween comprises:

encrypting the shared secret key with the public key of the application server to generate an encrypted shared key;

sending the encrypted shared secret key to the application server; and

decrypting the shared secret key with the private key of the application server.

7. The method of claim 5 wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol.

8. The method of claim 7 wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm.

9. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween utilizes a key agreement protocol.

10. The method of claim 9 wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm.

00503222.051300

1 11. The method of securely transferring data between an application server and an agent of
2 the application server through a non-secure environment having a web-server and the agent, the
3 method comprising:

- 4 a) a user accessing the web-server to download the agent therefrom; wherein the agent
5 includes a public key of the application server;
- 6 b) the agent establishing a shared session key with the application server by using the
7 public key of the application server, the shared session key for use in encrypting
8 and decrypting data to be transferred between the agent and the application
9 server;
- 10 c) the application server establishing a connection to the web-server; and
- 11 d) the agent contacting the web server by using a first protocol to send data encrypted by
12 the session key to the application server over the connection between the web-
13 server and the application server.

1 12. The method of claim 11 wherein the application server establishing a connection to the
2 web-server further comprises

- 3 c1) the application server dynamically instantiating a relay module by sending a URL
4 associated with the relay module to the web-server, the URL specifying a first
5 predetermined port for communication between the web-server and the relay
6 module;
- 7 c2) the application server connecting to the relay module on a first predetermined port;
8 and
- 9 c3) the application server reading data from the relay module through the connection on
10 the first predetermined port.

1 13. The method of claim 12 wherein the agent contacting the web server by using a first
2 protocol to send data encrypted by the session key to the application server over the connection
3 between the web-server and the application server further comprises

00592322.061300

- 4 d1) the agent encrypting the session key with the public key of the application server;
5 d2) the agent collecting data;
6 d3) the agent encrypting the collected data with the session key;
7 d4) sending the encrypted session key and encrypted measured data to the application
8 server by using a forwarding module that connects to a second predetermined port
9 of the relay module.

10
1 14. The method of claim 11 wherein the first protocol is one of HTTP and HTTP/SSL.

1 15. A secure data transfer system for connecting a non-secure node to an application server
2 behind a firewall comprising:

- 3 a) a web-server in the non-secure node;
4 b) a relay in the non-secure node that is dynamically instantiated by the application
5 server, the relay having a first port for listening for a connection from the
6 application server;

7 wherein the application server connects to the relay on the first port and reads data from
8 the first port.

1 16. The secure data transfer system of claim 15 further comprising:

- 2 a) an instantiation module for instantiating the relay module in response to an URL
3 associated with the relay module.

4
1 17. A secure data transfer system for establishing an end-to-end secure connection between
2 an agent and an application server behind a firewall through a non-secure node comprising:

- 3 a) a web-server residing in the non-secure node, the web-server having the agent that
4 includes a public key of the application server;

09592322-061300

- b) a browser in communication with the web-server for downloading the agent from the web-server;
- c) a secure transfer module residing in the non-secure node; and
- d) an application server in a secure zone for initiating a connection to the web-server via the secure transfer module.

18. The secure data transfer system of claim 17 wherein the secure transfer module further comprises:

- c1) a relay module for listening to a first port and a second port;
- c2) an instantiation module for executing the relay module in response to a command from the application server;
- c3) a forwarding module for transferring data from the agent to the relay module in response to a command from the agent; and

wherein the relay module listens to the first port for a connection by the application server and listens to the second port for a connection by the forwarding module.

19. The secure data transfer system of claim 16 wherein the non-secure node is a web-server node.

00592322.061300